WHITE PAPER

SECURE APPS FOR THE ENTERPRISE

A Practical Guide for Securing and Mobilizing Your Enterprise Apps

vmware®

Table of Contents

New Challenges for IT

In today's highly mobile world, employees can work from just about anywhere using just about any device. Gone are the days when the vast majority of employees worked in corporate buildings using stationary desktop systems loaded with applications and operating systems installed by IT administrators.

For your IT organization, this shift to the era of remote and mobile workers brings new challenges. The top-down, prescriptive model of pushing one-size-fits-all images to employees using standard hardware configurations is no longer viable. You now need to think in terms of securing and mobilizing enterprise applications, and that means long-used processes and management tools have to change, including the requirement for all employees to use the same types of devices.

Many employees now bring their own devices to their jobs, and increasingly departments and lines of business want to choose the latest form factor of a device, regardless of platform. These trends create the need for IT to support many device types, operating systems, and ownership models—from corporate-owned locked-down and shared devices to employees' personal devices. And all the while, a mobile workforce and a device-agnostic model create the need for new processes to deliver the apps and data that employees rely on to get their work done, wherever they are.

Security, too, is a huge concern when your IT organization is providing services to remote and mobile workers. You now need new strategies to protect corporate data at rest, in transit, and cached or stored on mobile devices.

So how do you secure and mobilize enterprise apps in this new era? In this paper, you'll learn about the unique approach VMware takes to secure application and access management.

Securing and Mobilizing Enterprise Apps

Bridging the Old and the New

A digital workspace platform provides the necessary tools to enable your IT organization to manage and secure diverse end-user devices and to deliver apps and data to remote and mobile employees.

A digital workspace platform goes beyond the capabilities of legacy XenApp, Remote Desktop Services (RDS), or virtual desktop infrastructure (VDI) and beyond the delivery of virtualized apps to remote users. It couples the delivery of virtualized apps and desktops with a consumer-simple experience and enterprise-class security. And it helps your organization bridge legacy client/server applications written for the PC era with new cloud-based, or native, mobile, cross-platform applications that require little endpoint dependence.

THE DIGITAL WORKSPACE

A digital workspace strategy enables your IT organization to deliver apps and data to employees across any device. With this new approach to the way end-user services are delivered, you can:

- Enable access to corporate owned, locked-down, and shared devices, as well as employees' personal devices with privacy protection.
- Protect corporate data at rest and in transit, including email, files, and application state that may be cached or stored on devices.
- Deliver native applications to devices and act as a contextual access manager for cloud-based and on-premises applications.
- Simplify employee onboarding and reduce the need for help-desk assistance.

Taking Control of Security

Centralizing and delivering virtual apps should be part of any security arsenal to help ensure that sensitive data is not stored on unsecure devices and those devices are kept off corporate networks, eliminating the risk and complexity of VPNs. However, modern security best practices can't simply rely on a "deep moat and a heavily guarded drawbridge" for security. Modern security demands that planners assume malicious code and bad actors will get through firewalls, whether apps are running on-premises or in the cloud.

VMware helps you overcome these challenges with the capabilities built into VMware Horizon® and VMware Workspace ONE™. Together, these software products give you the ability to keep your most sensitive data off devices and rogue devices out of the network.

The VMware platform helps you:

- **Eliminate the need for VPNs.** Pass only user-experience traffic, such as graphics and keystrokes, through a reverse proxy to limit exposure of local device malware to the corporate network.
- **Harden the network for "east-west" traffic.** Leverage VMware NSX® network virtualization that isolates individual apps, limiting malicious damage.
- **Implement fine-grained policies.** Use enable or restrict options, including printing or saving to local drives, based on properties such as device type, network location, and trust level of the device.
- **Increase security across your enterprise.** You can treat every device as hostile and secure apps the same way for every employee.

By keeping data off insecure devices and applying network micro-segmentation to each virtual workload, VMware helps your IT organization reduce attack risk and prevent data loss—while meeting the remote access needs of an increasingly mobile workforce.

A Comprehensive Solution

When you work with VMware for your digital workspace solution, you can have the confidence that comes with an end-to-end solution, including tight integration with your data center, advanced management technologies, and just-in-time management platform.

Tight Integration with the Software-Defined Data Center

To gain the full benefits of automation and workload portability across data centers and the cloud, you need a complete foundation of compute, storage, and network virtualization with management tools that span the stack.

As a global leader in cloud infrastructure and the digital workspace, VMware tightly integrates the desktop and app virtualization management of VMware Horizon with the compute (VMware vSphere®), storage (VMware vSAN™), and network (VMware NSX) virtualization technologies that form the core of the Software-Defined Data Center.

Advanced Management Technologies

The VMware digital workspace platform builds in advanced management technologies that deliver maximum flexibility and customization with superior TCO for application and desktop delivery, cutting common number of tasks and management time in half over leading competitors.

An Industry-First, Just-in-Time Management Platform

VMware Horizon is a just-in-time management platform that includes three key technologies untangling the OS, apps, and user personalization challenge: VMware Instant Clones, VMware App Volumes™, and VMware User Environment Manager™. Working together, these technologies deliver maximum flexibility and customization with superior TCO for application and desktop delivery, cutting common number of tasks and management time in half over leading competitors.[1]

> **VMware Workspace ONE** is a simple and secure enterprise platform that delivers and manages any app on any smartphone, tablet, or laptop. By integrating identity management, real-time application delivery, and enterprise mobility management, Workspace ONE engages digital employees, reduces the threat of data leakage, and modernizes traditional IT operations for the mobile cloud era.
>
> **VMware NSX** is a network virtualization and security platform that enables the creation of entire networks in software and embeds them in the hypervisor layer, abstracted from the underlying physical hardware. All network components can be provisioned in minutes, without the need to modify the application.
>
> **VMware Horizon** delivers virtualized or hosted desktops and applications through a single platform to end users. These desktop and application services—including RDS published apps, packaged apps with VMware ThinApp®, SaaS apps, and even virtualized apps from Citrix—can all be accessed with Workspace ONE, a single digital workspace that spans devices, locations, media, and connections, all without compromising quality and user experience.

1. From VMware contracted independent testing conducted with the release of Horizon 7.1, February 2017.

With Workspace ONE, customers not only stand to benefit from all of the recent innovations and integrations made across each of the individual product lines (Horizon, VMware AirWatch®, and Identity Manager™) but can also purchase a SKU with the mix of solutions that

2. IDC MarketScape: Worldwide Virtual Client Computing Software 2016 Vendor Assessment, November 2016.

Key Takeaways

- The VMware digital workspace platform helps you overcome the IT challenges brought by a growing number of mobile and remote workers.
- This digital workspace platform provides the necessary tools to enable your IT organization to manage and secure diverse end-user devices and to deliver apps and data to remote and mobile employees.
- By keeping data off unsecure devices and applying network micro-segmentation to each virtual workload, VMware helps reduce risk of attack and prevent data loss.

GET STARTED TODAY

Learn more about securing and mobilizing your apps.
Register for VMware Workforce Mobility Fundamentals.

Join Us Online:

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com